

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-151627

(43)Date of publication of application : 30.05.2000

(51)Int.Cl.

H04L 12/28
H04L 12/56

(21)Application number : 10-315732

(71)Applicant : CHOKOSOKU NETWORK COMPUTER GIJUTSU
KENKYUSHO:KK

(22)Date of filing : 06.11.1998

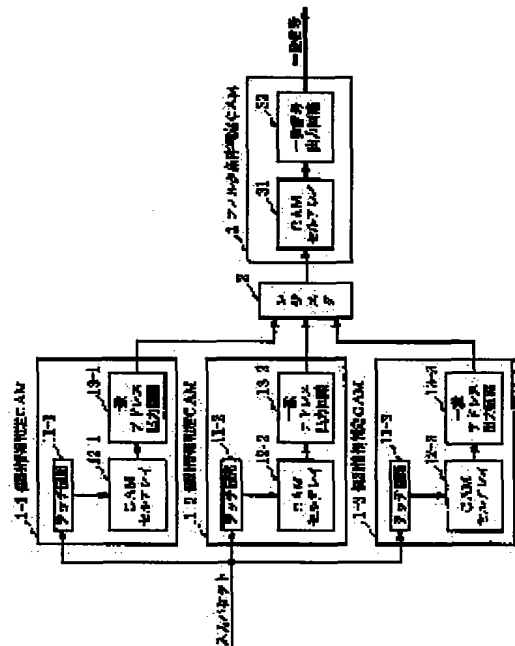
(72)Inventor : NOJIMA SATOSHI

(54) PACKET FILTER CIRCUIT

(57)Abstract:

PROBLEM TO BE SOLVED: To suppress increase in hardware volume by realizing high speed processing performance.

SOLUTION: Individual information discrimination CAMs (contents retrieval memories) 1-1, 1-2, 1-3 are provided to each type of various information configuring packet filter conditions. Coincident address output circuits 13-1, 13-2, 13-3 output an address of a coincident entry when an entry storing information coincident with information of an input packet. A CAM cell array 31 stores a set of coincident entry addresses as the packet filter conditions. A coincident signal output circuit 32 outputs a coincidence signal when the set of the coincident entry addresses outputted from a register 2 is coincident with the packet filter conditions of the CAM cell array 31.



LEGAL STATUS

[Date of request for examination] 06.11.1998

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3028414

[Date of registration] 04.02.2000

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right] 04.02.2003

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2000-151627

(P2000-151627A)

(43)公開日 平成12年 5月30日 (2000.5.30)

(51)Int.Cl.⁷

識別記号

F I

テーマコード(参考)

H 0 4 L 12/28
12/56

H 0 4 L 11/00
11/20

3 1 0 D 5 K 0 3 0
1 0 2 D 5 K 0 3 3

審査請求 有 請求項の数 3 O L (全 6 頁)

(21)出願番号 特願平10-315732

(22)出願日 平成10年11月 6 日(1998. 11. 6)

(71)出願人 394025577

株式会社超高速ネットワーク・コンピュータ技術研究所

東京都港区虎ノ門五丁目 2 番 6 号

(72)発明者 野島 聡

東京都港区虎ノ門 5 丁目 2 番 6 号 株式会社超高速ネットワーク・コンピュータ技術研究所内

(74)代理人 100064621

弁理士 山川 政樹

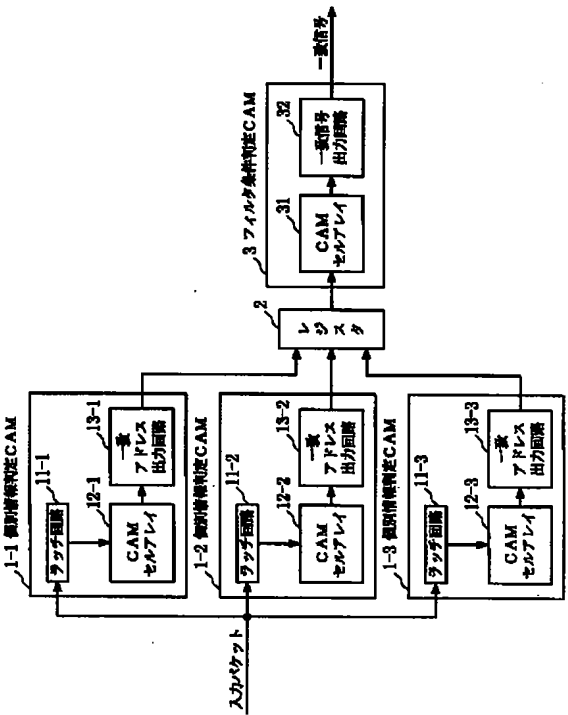
F ターム(参考) 5K030 GA01 GA05 HA08 HD03 HD09
JL07 KA05 KA13 KX24 LE09
5K033 CO01 DB01 DB12 DB18 EC04

(54)【発明の名称】 パケットフィルタ回路

(57)【要約】

【課題】 高速な処理性能を実現し、ハードウェア量の増大を抑制する。

【解決手段】 個別情報判定CAM(内容検索型メモリ) 1-1, 1-2, 1-3は、パケットフィルタ条件を構成する各種情報の種別毎に設けられる。一致アドレス出力回路 13-1, 13-2, 13-3は、入力パケットの情報と一致する情報を保持しているエントリが存在するとき、一致エントリのアドレスを出力する。CAMセルアレイ 31は、一致エントリアドレスの集合をパケットフィルタ条件として格納する。一致信号出力回路 32は、レジスタ 2から出力された一致エントリアドレスの集合がCAMセルアレイ 31のパケットフィルタ条件と一致したとき、一致信号を出力する。



【特許請求の範囲】

【請求項 1】 ネットワーク間でパケット中継を実現するパケット中継装置において、入力パケットの転送あるいは廃棄を決定するために入力パケットの属性を判断するパケットフィルタ回路であって、パケットフィルタ条件を構成する各種情報の種別毎に設けられ、該当種別の情報を格納するエントリを備え、各エントリに格納された情報と入力パケットが有する該当種別の情報とを比較して、一致する情報を格納しているエントリが存在するとき、この一致エントリのアドレスを出力する複数の第 1 の内容検索型メモリと、各種情報の集合からなるパケットフィルタ条件の代わりに、これら情報を格納している第 1 の内容検索型メモリの一致エントリアドレスの集合をパケットフィルタ条件として記憶し、複数の第 1 の内容検索型メモリからそれぞれ出力された一致エントリアドレスの集合がパケットフィルタ条件と一致したとき、一致信号を出力する第 2 の内容検索型メモリとを有することを特徴とするパケットフィルタ回路。

【請求項 2】 ネットワーク間でパケット中継を実現するパケット中継装置において、入力パケットの転送あるいは廃棄を決定するために入力パケットの属性を判断するパケットフィルタ回路であって、パケットフィルタ条件を構成する各種情報の種別毎に設けられ、該当種別の情報を格納するエントリを備え、各エントリに格納された情報と入力パケットが有する該当種別の情報とを比較して、一致する情報を格納しているエントリが存在するとき、この一致エントリの情報を表すコードを出力する複数の第 1 の内容検索型メモリと、各種情報の集合からなるパケットフィルタ条件の代わりに、これら情報を表すコードの集合をパケットフィルタ条件として記憶し、複数の第 1 の内容検索型メモリからそれぞれ出力されたコードの集合がパケットフィルタ条件と一致したとき、一致信号を出力する第 2 の内容検索型メモリとを有することを特徴とするパケットフィルタ回路。

【請求項 3】 請求項 1 又は 2 記載のパケットフィルタ回路において、複数の第 1 の内容検索型メモリの出力を所定の順序に配列して、これを第 2 の内容検索型メモリに与えるレジスタを有することを特徴とするパケットフィルタ回路。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ネットワーク間を接続するゲートウェイ装置等のパケット中継装置に係り、特にある一定の条件を満たすパケットを転送あるいは廃棄するというパケットフィルタ機能を実現するパケットフィルタ回路に関するものである。

【0002】

【従来の技術】 従来より、ネットワーク間を接続するゲ

ートウェイ装置等のパケット中継装置においては、IP アドレス、MAC アドレス、TCP ポート番号等々の、パケットヘッダに格納されている各種の情報を用いて、その各々がある一定の条件（パケットフィルタ条件）を満足した場合に、該パケットを転送あるいは廃棄するというパケットフィルタ機能が必要とされる。

【0003】 このフィルタ判別は、以下の要件を要求する。

(A) パケットフィルタ条件は、IP アドレス、MAC アドレス、TCP ポート番号等の各種情報のベクトル条件（集合）で設定される場合が一般的である。

(B) パケットフィルタ条件を構成する各種情報は、ゲートウェイ装置の場合の常として、長いビット長（例えば、IP アドレスで 32 ビット）を持つが、ある箇所のゲートウェイ装置では、そのビット長が示す数値空間の中で狭い数量しか必要としない。

【0004】 パケットフィルタ回路を構成する上での問題は、それぞれの情報の持つ数値空間全体に対して、必要とされる条件エントリの数は微小であり、有効な構成物量で必要な条件エントリを保持、検索させることが困難なことである。また、上述のように、パケットフィルタ条件は各種情報のベクトル条件であるため、入力パケットがパケットフィルタ条件を満たすか否かを判定するには、必要な全ての組み合わせを記憶した上で比較判定することが必要となり、この場合、上記した構成物量の無駄はより大きな問題を引き起こす。

【0005】 従来は、このようなパケットフィルタの構成の多くはソフトウェアに依存し、パケットフィルタ条件を具現化する判断分岐（フローチャート）を処理することで実現される。ハードウェアによる構成の場合には、各種情報の必要な全ての組み合わせを記憶した内容検索型メモリ（Content Addressable Memory、以下、CAM とする）の利用が考えられる。

【0006】 図 4 は CAM を利用した従来のパケットフィルタ回路のブロック図である。図 4 の例では、IP アドレスと MAC アドレスと TCP ポート番号の集合からパケットフィルタ条件が構成される場合を示し、CAM 41 の 1 行が 1 つのパケットフィルタ条件を格納したエントリとなっている。このように判定に必要な全てのパケットフィルタ条件を CAM 41 のエントリに格納した形となっている。よって、IP アドレスが同じであっても、MAC アドレスあるいはポート番号が異なるパケットフィルタ条件を設定する必要がある場合には、異なるエントリを CAM 41 に設ける必要がある。つまり、パケットフィルタ条件を構成する個別の情報に重複するものがあつたとしても、パケットフィルタ条件の総数と等しいエントリ数が必要となる。

【0007】 図 4 の例では、パケットフィルタ条件を IP アドレスと MAC アドレスと TCP ポート番号の 3 種類からなるものとしたが、通常、より多種の情報（アド

3

レスであれば、送信元アドレス、受信先アドレスの2種類などが要求される。よって、CAM41の1エントリが更に長くなることが予想され、現状実現されているCAMのエントリビット長が64から128程度であることを考慮した場合、十分なパケットフィルタ条件を設定することは困難である。

【0008】

【発明が解決しようとする課題】 以上のように、パケットフィルタをソフトウェアで実現した場合、複数のパケットフィルタ条件と入力パケットとの比較判定がシリアルで処理されるため、多くの処理ステップが必要となり、処理に時間がかかるという問題点があった。また、パケットフィルタをCAM等のハードウェアで実現した場合、非常に長いワード（エントリ）長を必要とし、多くのハードウェア量を必要とするという問題点があった。本発明は、上記課題を解決するためになされたもので、ソフトウェア処理よりも高速な処理性能を実現すると共に、ハードウェア量の増大を抑制することができるパケットフィルタ回路を提供することを目的とする。

【0009】

【課題を解決するための手段】 本発明のパケットフィルタ回路は、請求項1に記載のように、パケットフィルタ条件を構成する各種情報の種別毎に設けられ、該当種別の情報を格納するエントリを備え、各エントリに格納された情報と入力パケットが有する該当種別の情報とを比較して、一致する情報を格納しているエントリが存在するとき、この一致エントリのアドレスを出力する複数の第1の内容検索型メモリと、各種情報の集合からなるパケットフィルタ条件の代わりに、これら情報を格納している第1の内容検索型メモリの一致エントリアドレスの集合をパケットフィルタ条件として記憶し、複数の第1の内容検索型メモリからそれぞれ出力された一致エントリアドレスの集合がパケットフィルタ条件と一致したとき、一致信号を出力する第2の内容検索型メモリとを有するものである。このように、第1の内容検索型メモリによってパケットフィルタ条件を構成する各種情報の種別毎に検索を行い、第2の内容検索型メモリによって第1の内容検索型メモリからの一致エントリアドレスの集合がパケットフィルタ条件と一致するか否かを判定することにより、入力パケットの属性を判断することができる。

【0010】 また、請求項2に記載のように、パケットフィルタ条件を構成する各種情報の種別毎に設けられ、該当種別の情報を格納するエントリを備え、各エントリに格納された情報と入力パケットが有する該当種別の情報とを比較して、一致する情報を格納しているエントリが存在するとき、この一致エントリの情報を表すコードを出力する複数の第1の内容検索型メモリと、各種情報の集合からなるパケットフィルタ条件の代わりに、これら情報を表すコードの集合をパケットフィルタ条件とし

4

て記憶し、複数の第1の内容検索型メモリからそれぞれ出力されたコードの集合がパケットフィルタ条件と一致したとき、一致信号を出力する第2の内容検索型メモリとを有するものである。このように、第1の内容検索型メモリによってパケットフィルタ条件を構成する各種情報の種別毎に検索を行い、第2の内容検索型メモリによって第1の内容検索型メモリからのコードの集合がパケットフィルタ条件と一致するか否かを判定することにより、入力パケットの属性を判断することができる。また、請求項3に記載のように、複数の第1の内容検索型メモリの出力を所定の順序に配列して、これを第2の内容検索型メモリに与えるレジスタを有するものである。

【0011】

【発明の実施の形態】 [実施の形態の1] 次に、本発明の実施の形態について図面を参照して詳細に説明する。図1は本発明の第1の実施の形態となるパケットフィルタ回路のブロック図である。本実施の形態のパケットフィルタ回路は、パケットフィルタ条件を構成する各種情報の種別毎に設けられた、個別情報判定CAM（第1の内容検索型メモリ）1-1、1-2、1-3を有している。

【0012】 各個別情報判定CAM1-1、1-2、1-3は、入力パケットのパケットヘッダから該当種別の情報（検索ワード）を抽出するラッチ回路11-1、11-2、11-3と、該当種別の情報（被検索ワード）を格納するための複数のエントリを有するCAMセルアレイ12-1、12-2、12-3と、ラッチ回路11-1、11-2、11-3から出力された情報と一致する情報を保持しているエントリが存在するとき、この一致エントリのアドレスを出力する一致アドレス出力回路13-1、13-2、13-3とから構成されている。

【0013】 個別情報判定CAM1-1は、パケットフィルタ条件を構成する各種情報のうちIP（Internet Protocol）アドレスに対応するものである。ラッチ回路11-1は、入力パケットのパケットヘッダからIPアドレスを抽出し、CAMセルアレイ12-1は、IPアドレスを被検索ワードとして格納している。一致アドレス出力回路13-1は、ラッチ回路11-1から出力されたIPアドレスと一致するIPアドレスを保持しているエントリがCAMセルアレイ12-1に存在するとき、この一致エントリのアドレスを出力する。

【0014】 個別情報判定CAM1-2は、パケットフィルタ条件を構成する各種情報のうちMAC（Media Access Control）アドレスに対応するものである。ラッチ回路11-2は、入力パケットのパケットヘッダからMACアドレスを抽出し、CAMセルアレイ12-2は、MACアドレスを被検索ワードとして格納している。一致アドレス出力回路13-2は、ラッチ回路11-2から出力されたMACアドレスと一致するMACアドレスを保持しているエントリがCAMセルアレイ12-2に

存在するとき、この一致エントリのアドレスを出力する。

【0015】個別情報判定CAM1-3は、パケットフィルタ条件を構成する各種情報のうちTCP (Transmission Control Protocol) ポート番号に対応するものである。ラッチ回路11-3は、入力パケットのパケットヘッダからTCPポート番号を抽出し、CAMセルアレイ12-3は、TCPポート番号を被検索ワードとして格納している。一致アドレス出力回路13-3は、ラッチ回路11-3から出力されたTCPポート番号と一致するTCPポート番号を保持しているエントリがCAMセルアレイ12-3に存在するとき、この一致エントリのアドレスを出力する。

【0016】以上のように、各個別情報判定CAM1-1, 1-2, 1-3は、それぞれが対応する情報に関しての一致検索を実施する。レジスタ2は、各個別情報判定CAM1-1, 1-2, 1-3から出力された一致エントリアドレスを所定の順序に配列するためのもので、各個別情報判定CAM1-1, 1-2, 1-3から出力された一致エントリアドレスをいったん格納し、これらを所定の順序で出力する。

【0017】次に、本実施の形態のパケットフィルタ回路では、従来のような各種情報の集合からなるパケットフィルタ条件の代わりに、これら情報を格納している各個別情報判定CAM1-1, 1-2, 1-3の一致エントリアドレスの集合をパケットフィルタ条件としている。

【0018】フィルタ条件判定CAM (第2の内容検索型メモリ) 3は、個別情報判定CAM1-1, 1-2, 1-3の一致エントリアドレスの集合をパケットフィルタ条件として格納するCAMセルアレイ31と、レジスタ2から出力された一致エントリアドレスの集合がCAMセルアレイ31のパケットフィルタ条件と一致したとき、一致信号を出力する一致信号出力回路32とから構成されている。

【0019】このように、本実施の形態では、個別情報判定CAM1-1, 1-2, 1-3により、パケットフィルタ条件を構成する各種情報の種別毎に検索を行い、各個別情報判定CAM1-1, 1-2, 1-3から出力された一致エントリアドレスをレジスタ2によって所定の順序に配列して、フィルタ条件判定CAM3に入力する。そして、フィルタ条件判定CAM3によってレジスタ2からの一致エントリアドレスの集合がパケットフィルタ条件と一致するか否かを判定することにより、入力パケットの属性を判断することができ、一致信号の出力に応じて入力パケットの転送あるいは廃棄を行うことができる。

【0020】なお、レジスタ2から出力される一致エントリアドレスの順序は、CAMセルアレイ31に格納された一致エントリアドレスの順序と同じであることは言

うまでもない。例えば、CAMセルアレイ31に格納されたパケットフィルタ条件がCAM1-1のエントリアドレス、CAM1-2のエントリアドレス、CAM1-3のエントリアドレスの順に設定されているとすれば、レジスタ2は、この順序で各個別情報判定CAM1-1, 1-2, 1-3からの一致エントリアドレスを出力する。

【0021】図2は本実施の形態のパケットフィルタ回路の動作を説明するための説明図である。図2において、個別情報判定CAM1-1, 1-2, 1-3及びフィルタ条件判定CAM3の各行は、エントリを示している。入力パケットのパケットヘッダにIPアドレス=c、MACアドレス=b、ポート番号=i i iが設定されていたとすると、個別情報判定CAM1-1, 1-2, 1-3からは一致エントリアドレスとして、それぞれアドレスma, mb, mcが出力される。このとき、フィルタ条件判定CAM3のCAMセルアレイ31にエントリアドレスma, mb, mcの組み合わせがパケットフィルタ条件として設定されていれば、一致信号出力回路32より一致信号が出力される。

【0022】〔実施の形態の2〕図3は本発明の第2の実施の形態となるパケットフィルタ回路のブロック図であり、図1と同一の構成には同一の符号を付してある。本実施の形態において、個別情報判定CAM1a-1, 1a-2, 1a-3内のCAMセルアレイ12a-1, 12a-2, 12a-3は、図1のCAMセルアレイ12-1, 12-2, 12-3と同様の情報とこの情報を表すコード (符号) とを各エントリに格納している。

【0023】符号出力回路14-1, 14-2, 14-3は、ラッチ回路11-1, 11, 2, 11-3から出力された情報と一致する情報を保持しているエントリがCAMセルアレイ12a-1, 12a-2, 12a-3に存在するとき、この一致エントリに格納されたコードを出力する。

【0024】本実施の形態のパケットフィルタ回路では、各種情報の集合からなるパケットフィルタ条件の代わりに、各種情報をコード化して、コードの集合をパケットフィルタ条件としている。フィルタ条件判定CAM3aは、コードの集合をパケットフィルタ条件として格納するCAMセルアレイ31aと、レジスタ2から出力されたコードの集合がCAMセルアレイ31aのパケットフィルタ条件と一致したとき、一致信号を出力する一致信号出力回路32aとから構成されている。その他の構成は、実施の形態の1と全く同じである。

【0025】

【発明の効果】本発明によれば、パケットフィルタ回路を内容検索型メモリというハードウェアで構成したので、ソフトウェア処理よりも高速な処理性能を実現することができる。また、第1の内容検索型メモリの各々は同一の情報を重複して持つ必要がなく、パケットフィル

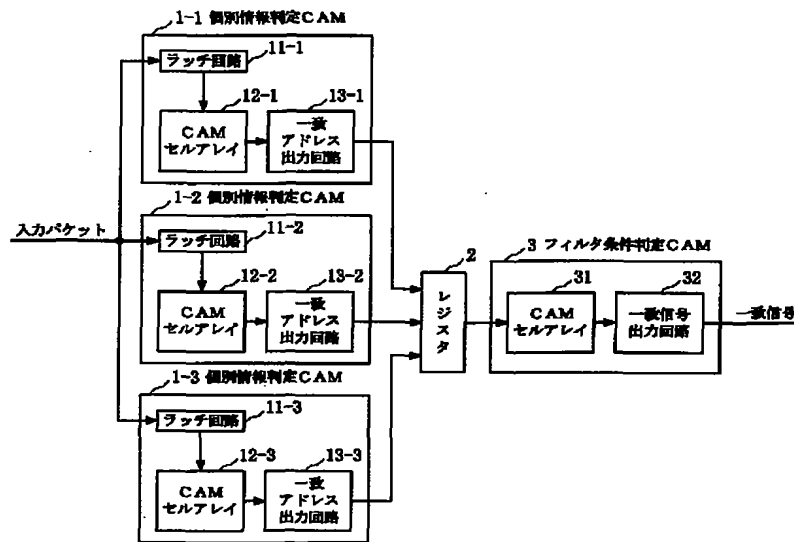
タ条件を構成する各種情報の種別毎に第1の内容検索型メモリを設けるため、パケットフィルタ条件が多種類の情報から構成される場合であっても、実現性が高く、従来のパケットフィルタ回路よりもハードウェア量を低減することができる。さらに、第2の内容検索型メモリは一致エントリアドレスの集合あるいは情報を表すコードの集合をパケットフィルタ条件として記憶するため、パケットフィルタ条件を表す必要ビット数が最低限度の量で事足りるので、ハードウェア量を更に低減することができる。

【図面の簡単な説明】

【図1】 本発明の第1の実施の形態となるパケットフィルタ回路のブロック図である。

【図2】 図1のパケットフィルタ回路の動作を説明するための説明図である。

【図1】



【図4】

41

IPアドレス対応	MACアドレス対応	ポート番号対応
IPアドレス=a	MACアドレス=b	ポート番号=i
IPアドレス=a	MACアドレス=b	ポート番号=iii
⋮	⋮	⋮
IPアドレス=b	MACアドレス=b	ポート番号=iii
⋮	⋮	⋮
IPアドレス=n	MACアドレス=m	ポート番号=iv

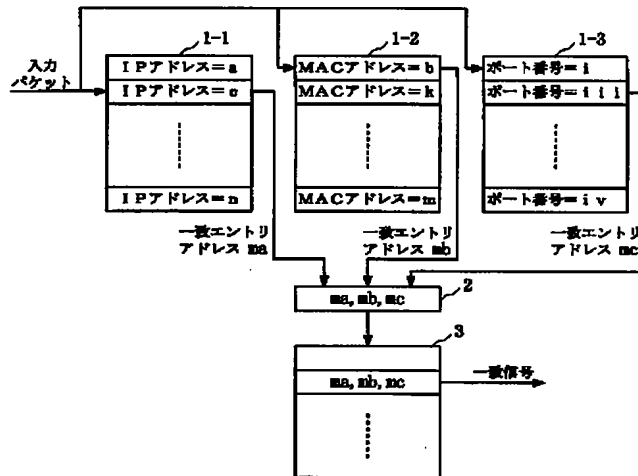
【図3】 本発明の第2の実施の形態となるパケットフィルタ回路のブロック図である。

【図4】 従来のパケットフィルタ回路のブロック図である。

【符号の説明】

1-1、1-2、1-3、1a-1、1a-2、1a-3…個別情報判定CAM、2…レジスタ、3、3a…フィルタ条件判定CAM、11-1、11-2、11-3…ラッチ回路、12-1、12-2、12-3、12a-1、12a-2、12a-3…CAMセルアレイ、13-1、13-2、13-3…一致アドレス出力回路、14-1、14-2、14-3…符号出力回路、31、31a…CAMセルアレイ、32、32a…一致信号出力回路。

【図 2】



【図 3】

